情報提供システムの最適化の実施に係る
仮想専用サーバ等一式

調達仕様書

独立行政法人　医薬品医療機器総合機構

平成２６年３月

目　次

1.　調達件名 1
2.　作業の概要 1
（1）　目的 1
（2）　用語の定義 1
（3）　業務の概要 2
（4）　調達の範囲 2
（5）　スケジュール 3
（6）　作業内容・納入成果物 4
（7）　検収 8
3.　技術要件 8
（1）　情報・データ要件 8
（2）　外部インタフェース要件 8
4.　規模・性能要件 8
（1）　規模要件 8
（2）　性能要件（参考情報） 9
5.　信頼性等要件 9
（1）　信頼性要件 9
（2）　拡張要件 １０
（3）　上位互換性要件 １１
（4）　システム中立性要件 １１
（5）　事業継続性要件 １１
6.　情報セキュリティ要件 １１
（1）　情報セキュリティ対策 １１
7.　情報システム稼動環境 １２
（1）　全体構成 １２
（2）　ハードウェア・ソフトウェア構成 １２
（3）　ネットワーク構成 １６
（4）　アクセシビリティ要件 １９
（5）　クラウド要件 １９
（6）　クラウドセンター施設設備要件 ２１
（7）　運用監視・保守要件 ２３
8.　作業の体制及び方法 ２３
（1）　作業体制 ２３
（2）　瑕疵担保責任 ２３
9.　特記事項 ２３
（1）　基本事項 ２３
（2）　入札制限 ２４
（3）　応札条件 ２４
（4）　知的財産等 ２４
（5）　再委託 ２５
（6）　機密保持 ２５
（7）　遵守事項 ２６
（8）　作業場所 ２６
（9）　環境への配慮 ２６
（１０）　その他 ２７
10.　留意事項 ２７

11.　窓口連絡先 ２７
別紙１：　セキュリティ脆弱性診断要件 １
別紙２：　セキュリティ対応方針と役割分担 ３
別紙３：　バックアップ・リカバリ方針 ７
別紙４：　運用監視・保守方針と役割分担 １１

1. 調達件名

情報提供システムの最適化の実施に係る仮想専用サーバ等一式

2. 作業の概要

（1） 目的

独立行政法人医薬品医療機器総合機構（以下「機構」という。）では、平成 19 年度に「業務・システム最適化計画」を策定し、これに基づき業務・システムの最適化の実施に係る各種システムの要件定義を行ってきたところである。

また、安全対策・健康被害救済関連システムについては、平成 22 年度から平成 23 年度において、業務・機能要件定義、サーバ機器・ネットワークインフラ等非機能要件に関する要件定義を実施してきた。

現在機構では、情報提供システムとして以下 2 つのウェブサイトを運営している。

① 独立行政法人医薬品医療機器総合機構ホームページ（http://www.pmda.go.jp/）（以下「コーポレートサイト」という。）

② 医薬品医療機器情報提供ホームページ（http://www.info.pmda.go.jp/）（以下「インフォサイト」という。）

要件定義において、IT を活用した質の高い情報提供実現に向けて、サイト構成等の要件取りまとめ及び戦略的な運営態勢の検討を実施してきた。

本調達はこの検討結果をうけ、機構による質の高い情報提供の実現に向けて、コーポレートサイトとインフォサイトの統合を中心とした情報提供システムの再構築（以下、再構築後のサイトを「次期コーポレートサイト」、サイトを構成するシステムを「本システム」という。）を行うために必要となるサーバ及びストレージ等ハードウェア、並びに OS 等ソフトウェア、インターネット回線及びネットワーク機器等について、必要となるライセンス費用を含む環境提供及びこれらに係る保守サービスを調達することを目的とする。

（2） 用語の定義

表 1　用語の定義

用　語	定　義
添付文書	医薬品においては、用法、用量その他使用及び取扱い上の必要な注意等の定められた事項を記載し、医薬品に添付される文書。医療機器においては、使用方法その他使用及び取扱い上の必要な注意等の定められた事項を記載し、医療機器に添付される文書。 薬事法にその根拠があり、医薬品、医療機器については添付文書の作成と添付が義務付けられている。
添付文書 SGML	添付文書の内容を SGML で記述したもの。システムにて管理されている。
ラインリスト	「症例一覧」「不具合一覧」の意。
次期コーポレートサイト	本業務で再構築された機構の情報提供システムの意。
専用サーバ	ホスティングにより提供される、機構が管理者権限を有することが可能なサーバ機器の意。

用　語	定　義
Virtual Private Server （VPS）	仮想環境上で提供される専用サーバの意。
Infrastructure as a Service （IaaS）	情報システムの稼働に必要な機材や回線などの基盤を、インターネット上のサービスとして遠隔から利用できるようにしたもの。
クラウド	ソフトウェアやハードウェアの利用権などをネットワーク越しにサービスとして利用者に提供する方式を「クラウドコンピューティング」(cloud computing)と呼び、データセンターや、その中で運用されているサーバ群のことをクラウドという

（３） 業務の概要

機構の中心業務である、審査関連業務、安全対策業務、健康被害救済業務では、それぞれの業務上広範囲への発信が必要な情報をコーポレートサイト又はインフォサイトに掲載している。

コーポレートサイトには、機構の紹介、審査に係る申請手続きの情報、健康被害救済制度の給付決定に関する情報等を掲載している。またインフォサイトには、添付文書やラインリスト等の安全対策に係る情報や承認情報等の情報を掲載している。

現在、コーポレートサイトの運営は企画調整部、インフォサイトの運営は安全第一部が実施している。サイト利用者は一般国民・医療機関・製薬会社及び医療機器メーカー・教育機関・研究機関等多岐にわたっている。なお、海外への情報発信を目的とした英語版ホームページはコーポレートサイトの１コンテンツとして含めている。

（４） 調達の範囲

本業務では、現在別途構築中の次期コーポレートサイトの稼働に必要となる環境提供等を行うものである。なお、下記事項に関する要件・仕様の詳細は別途調達済みの「情報提供システムの再構築に係る設計・開発等業務」において作成された「医薬品医療機器情報提供システム　HW／ＳW基本設計書」を参照すること。

本業務の範囲は以下の事項とする。

① クラウド環境提供
② ネットワーク回線の提供と敷設
③ ハードウェアの納入
④ ソフトウェアの納入
⑤ ネットワーク疎通確認
⑥ 本番環境構築支援
⑦ 結合・総合テストにおける作業支援
⑧ 移行・本番切替工程における作業支援
⑨ ハードウェア及びソフトウェアの保守
⑩ セキュリティ診断とその報告（年１回計７回程度を想定）

（５） スケジュール

① 作業スケジュール

本調達に係る業務全体の実施スケジュールの概要を以下に示す。

表 2　作業スケジュール

	25 年 11 月	12 月	26 年 1 月	2 月	3 月	4 月	5 月	6 月	7 月
（クラウド環境提供）									
機器等手配					→				
環境提供						→	→	→	→
テスト等支援							→	→	→
本番切替支援								→	→
（設計・開発）									
要件定義	→	→	→	→	→				
CMS 選定	→	→	→						
設計開発	→	→	→	→	→	→			
テスト					→	→	→	→	→
移行					→	→	→	→	→
運用開始									→

② 役割分担

本調達は、現在別途構築中の次期コーポレートサイトの稼働に必要となる環境提供等を発注するものであり、「設計・開発」及び別途調達予定の「運用・保守」については本調達の対象外とする。なお、下表の各調達単位の受託業者をそれぞれ「設計・開発業者」、「本件受注者」、「運用・保守業者」という。

表 3 役割分担

項番	作業項目	分担		
		受注者 ※本調達	設計・ 開発業者 ※別途 調達済	運用・ 保守業者 ※別途 調達予定
1	クラウド環境提供	○		
2	クラウド環境設計		○	
3	ネットワーク回線提供・敷設	○		
4	ネットワーク回線疎通確認	○		
5	ハードウェア・ソフトウェア納入	○		
6	ハードウェア・ソフトウェア保守	○		
7	本番環境構築		○	
8	本番環境構築支援	○		
9	テスト・移行		○	
10	テスト・移行作業支援	○		
11	本番切替		○	
12	本番切替作業支援	○		
13	本システム運用・保守			○

（６） 作業内容・納入成果物

本調達は、ネットワークを含む次期システムの稼働環境の提供等を発注するものであり、具体的な業務及び納入成果物は下記に示すとおりである。納入成果物の構成、詳細については、受注後、機構と協議し取り決めること。

① 作業内容等

ア．プロジェクト実施計画書の作成

後述の作業を実施するにあたりプロジェクト実施計画書を作成すること。実施計画書の記載内容については、機構及び設計・開発業者と協議し、修正が必要な場合には本件受注者は修正を実施すること。

イ．クラウド環境の提供

本システムを稼働するためのクラウド環境を提供すること。クラウド環境には仮想化サーバ、仮想化ストレージ、仮想化ネットワークを含むこと。

標準で運用・監視サービスも含むこと。

ウ．ネットワーク回線の提供と敷設

以下に示す本システムに必要なネットワーク回線を提供、敷設、結線すること。

- インターネット回線
- VPN 接続環境（クラウド環境～機構間、及び機構間～新システム検証環境間）及び必要となる機器等

インターネット回線についてはインターネットサービスプロバイダ及び本システムに必要なグローバル IP アドレスの提供も含むものとする。

なお、本調達外で回線敷設が発生した場合、回線敷設作業は各調達の落札業者が実施するが、その際の必要な情報提供、支援作業を実施すること。

エ．ハードウェアの納入

以下に示す本システムに必要となるハードウェアを納入すること。

- VPS（クラウド環境）
- ネットワーク機器（VPN 回線に必要となる機器）

個々の要件の詳細は「7　情報システム稼働環境」を参照のこと。

オ．ソフトウェアの納入

以下に示す本システムに必要となるソフトウェアを納入すること。

- 基本ソフトウェア（OS）
- ミドルウェア、パッケージソフトウェア

ソフトウェア要件の詳細は「7　情報システム稼働環境」を参照のこと。

カ．ネットワークの疎通確認

本件受注者は、提供、敷設する全てのネットワーク回線の疎通確認作業を実施すること。実施にあたっては動作確認計画書及び動作確認結果報告書を作成すること。動作確認計画書の記載内容については、機構、及び設計・開発業者と協議し、修正が必要な場合には本件受注者は修正を実施すること。

キ．本番環境構築支援

本番環境は一から構築するのではなく、設計・開発業者が別途構築している新システム検証環境上に構築された仮想環境の資産を有効活用することを想定している。このため、検証環境上に構築された仮想環境を容易に移設可能となるよう、VMware 社の VMwareESX 及び Redhat 社の KVM から、提供するクラウド環境への移行ツール等の提供が可能であり、設計・開発業者から当該ツールに係る支援の要請があった場合は、実機への作業を含み支援対応を行うこと。

ク．結合・総合テストにおける作業支援

本件受注者は、設計・開発業者が実施する結合・総合テストにおいて、設計・開発業者から以下の支援の要請があった場合には、実機での作業も含み支援対応を行うこと。なお、本件受注者は、設計・開発業者が実施する結合・総合

テストの進捗に遅延をきたさないような作業支援体制等を考慮すること。

- ハードウェア、ソフトウェア、ネットワークの不具合に関する動作状態の確認・解析支援
- ハードウェア、ソフトウェア、ネットワークの各種設定情報の確認・変更支援
- その他協力が必要となった場合の支援

ケ．移行・本番切替工程における作業支援

移行工程は設計･開発業者が主体となり各移行工程を進捗するが、本件受注者は、設計･開発業者が実施する移行テスト、リハーサル及び回線切替前に実施する本番切替作業において、設計・開発業者から次の支援の要請があった場合は、実機への作業を含み支援対応を行うこと。

- ハードウェア、ソフトウェア、ネットワークの不具合に関する動作状態の確認・解析支援
- ハードウェア、ソフトウェア、ネットワークの各種設定情報の確認・変更支援
- その他協力が必要となった場合の支援

コ．ハードウェア及びソフトウェアの保守

以下に示す本システムに必要な機構内に設置するハードウェアに関する保守を提供すること。

- VPS（クラウド環境）
- ネットワーク機器（VPN 回線に必要となる機器）

個々の要件の詳細は「7　情報システム稼働環境」を参照のこと。

同様に、以下に示す本システムに必要なソフトウェアに関する保守を提供すること。

- 基本ソフトウェア（OS）
- ミドルウェア、パッケージソフトウェア

ソフトウェア要件の詳細は「7　情報システム稼働環境」を参照のこと。

サ．セキュリティ診断とその報告

年１回（計７回程度を想定）本システムにおけるセキュリティ監査のためのネットワーク診断及び Web 脆弱性診断を実施し、報告書を提出すること。診断要件の詳細は別紙１「セキュリティ脆弱性診断要件」を参照のこと。

② 納入成果物

作業工程毎に求める納入成果物は下表に示すとおり。

表 4 納入成果物

項番	工程	納入成果物	納入期日
1	計画	プロジェクト実施計画書	契約締結から 2 週間以内
2	導入・設置	機器及びソフトウェア等一式	平成 26 年 4 月上旬
3	導入・設置	納入する機器及びソフトウェア取扱説明書	平成 26 年 4 月上旬
4	導入・設置	納入物品一覧（製品名、メーカー、製造番号、シリアル番号、納入数を記載）	平成 26 年 3 月末
5	導入・設置	ネットワーク機器配線図等	平成 26 年 4 月上旬
6	導入・設置	動作確認計画書、動作確認結果報告書	平成 26 年 4 月上旬
7	その他	打合せ資料、議事録	随時
8	その他	支援実施報告書	平成 26 年 7 月末
9	保守	セキュリティ診断報告書	別途調整

なお、納入成果物については、以下の条件を満たすこと。

ア．文書は、今回改修に該当する開発箇所及び操作説明書、各報告書については、紙及び磁気媒体等（CD-R 又は CD-RW 等）により日本語で提供すること。

イ．紙のサイズは、日本工業規格 A 列 4 番を原則とする。図表については、必要に応じて A 列 3 番縦書き、横書きを使用することができる。バージョンアップ時等に差換えが可能なようにバインダー方式とする。

ウ．磁気媒体等に保存する形式は、PDF 形式又は Microsoft Office2007 で扱える形式とする。ただし、機構が別に形式を定めて提出を求めた場合は、この限りではない。

エ．紙及び磁気媒体については二部ずつ用意すること（作成プログラムは一式）。

③ 想定利用期間

契約後取り決めた稼働開始日 ～ 平成 31 年 3 月 31 日

個別に納入する機器の保守対応期間も同様とする。

④ 納入場所

独立行政法人 医薬品医療機器総合機構 情報化統括推進室

（所在地：東京都千代田区霞が関 3-3-2 新霞が関ビル 10F）

但し、クラウド環境については本件受注者の提供するサービスの稼動する日本国内のデータセンターとする。

⑤ 納入期限

平成 26 年 7 月 31 日

（クラウド環境提供期限は平成 26 年 4 月 ※契約後別途定める）

（７） 検収

納入成果物については、適宜、機構に進捗状況の報告を行うとともに、レビューを受けること。最終的な納入成果物については、「表４　納入成果物」に記載のすべてが揃っていること及びレビュー後の改訂事項等が反映されていることを、機構が確認し、これらが確認され次第、検収終了とする。

なお、以下についても遵守すること。

① 検査の結果、納入成果物の全部又は一部に不合格品を生じた場合には、受注者は直ちに引き取り、必要な修復を行った後、機構の承認を得て約束した日時までに修正が反映されたすべての納入成果物を納入すること。

② 「表４　納入成果物」に規定されたもの以外にも、必要に応じて提出を求める場合があるので、作成資料等を常に管理し、最新状態に保っておくこと。

3. 技術要件

（１） 情報・データ要件

「４　規模・性能要件」のデータボリュームを参照のこと。また、これによらず設計・開発業者と十分な連携をとること。

（２） 外部インタフェース要件

本システムは、外部の現行システムデータセンターと夜間処理等で連携し、また新システム検証環境とも連携するため、設計・開発業者と十分な連携をとること。

4. 規模・性能要件

（１） 規模要件

以下に規模要件を示す。規模要件は運用開始後５年後の推定値である。クラウドサービスとして下記要件を満たす構成を提供すること。但し、想定外のアクセス量、データ量発生時にも、必要に応じリソースを拡張し対応していくことが可能であること。

① 利用者数

一般公開での利用者数：
平成 22 年末調査時点で最大 86,000 名強
2 倍程度まで増加すると推定し 172,000 名程度
機構内での利用者数：150 名程度

② 業務量

1 日当たりのコンテンツ掲載件数：20 件程度

③ データボリューム

データ容量：約 2.0TB
ファイル数：平成 22 年度末調査時点で 85,000 ファイル（html、PDF)。
3 倍程度まで増加すると推定し、255,000 ファイル（html、PDF)。

（２） 性能要件（参考情報）

以下に性能要件を示す。

① 一般公開での目標スループット

ア．目標スループット（同時利用者数）は 60 とする。平成 23 年の 1 日最多ページビュー数が約 34 万であり、ピーク時間帯（5 時間）に集中すると想定した場合、同時利用者数は約 20 となる。同時アクセス数増大率を 3 倍とした。

イ．目標トランザクション数は約 100 万ページビュー／日とする。上記 1 日最多ページビュー数をトランザクション数とし、増大率を 3 倍とした。

② 機構内管理機能における性能要件

ア．画面応答（参照系処理）は 3 秒以内とする。

イ．画面応答（更新系処理）は 10 秒以内とする。（※1）

ウ．DB 検索結果表示は 10 秒以内とする。（※1）

エ．DB 更新処理は 10 秒以内とする。（※1）

オ．文書ファイル（PDF 又は Word ファイルを想定。以下同じ。）表示は 10 秒以内とする。（※2）

カ．文書ファイル検索結果応答は 10 秒以内とする。（※1）

キ．文書ファイル全文検索結果応答は 30 秒以内とする。（※1）

ク．ファイルの更新処理（新旧ファイルの差替え処理、出力処理など）は 1 分以内とする。（※3）

上記は、VPN 等を経由したアクセス時や、件数・容量が大きい場合の許容限界である。許容限界を超えるような機能が必要な場合は機構と協議の上、別途適切に定めること。許容限界を超える機能の要因として、対象データが膨大となる場合や検索条件が索引を使えないような複雑な場合などを想定している。

※1：通常は、3 秒以内とする。

※2：通常は、5 秒以内とする。

※3：通常は、10 秒以内とする。

5. 信頼性等要件

（１） 信頼性要件

① ストレージ

ア．データファイルは信頼性の高い外部ストレージに配置すること。

イ．ストレージ装置について、可能な限りコントローラ、電源、FAN、I/F 等を冗長構成とすること。

ウ．データのバックアップは、サービス提供時間及び RPO（目標復旧時点）／RTO（目標復旧時間）との兼合いから、オンラインバックアップ方式とする。

エ．原則、システム内の全データは、「外部システム、外部データ、人手」に依存することなく復旧が可能となるに必要なバックアップを取得すること。

② ネットワーク

ア．LAN 及び SAN は原則、すべての経路・機器ともに 2 重化すること。

イ．ネットワーク機器は原則、すべてのコンポーネント（電源、CPU、FAN、I/F 等）を冗長化すること。

ウ．Web サーバ等既存アプリケーションに影響を及ぼす可能性がある箇所はロードバランサをトランスレータとして利用すること。

エ．サービスの提供時間が計画停止時間を除き、24 時間年中無休であること。

③ 障害時に許容できるサービス停止時間等

ア．大規模災害を除く業務停止時において、6 時間以内に復旧できることを目標とする。

イ．Web 系システムは、ロードバランサを導入し、冗長性を高めることで業務停止につながる障害を抑えつつ、共有コンテンツのリストア等、長時間の処理を行う必要がないものについては、2 時間以内を目標になるべく早く復旧する。ただし、サービスレベルとして保証する数値とはしない。

（２） 拡張要件

拡張性要件を以下に示す。

① システムの利用期間

機器は 5 年程度（メーカーの交換部品保証期間）の利用を想定する。

② データ拡張

5 年後のデータ容量は、約 2TB と推定している。推定下限容量のストレージ実行領域を用意し、上限までのオンライン拡張可能な構成を検討すること。

③ 利用者拡張

一般公開での利用者数は 172,000 名程度（平成 22 年末調査時点で最大 86,000 名強であり、2 倍程度まで増加すると推定）と想定している。また、機構内での利用者数は 100 名程度である。

④ 機器の拡張

利用者数増加によるアクセス負荷の増大を考慮して、将来的にサーバの追加、CPU、HDD、メモリの増設が可能な構成とすること。

表 5 拡張対象機器一覧

項番	対象機器	拡張方式	内容
1	共有コンテンツサーバ	スケールアップ	CPU、MEM、HDD
2	インタフェースサーバ		CPU、MEM、HDD
3	改ざん検知サーバ		CPU、MEM、HDD
4	事前公開兼検証用 Linux サーバ		CPU、MEM、HDD

項番	対象機器	拡張方式	内容
5	検証用 Windows サーバ		CPU、MEM、HDD
6	ファイアウォール		処理能力
7	ロードバランサ		処理能力
8	オンラインストレージ		ディスク容量
9	Web/AP サーバ	スケールアウト	台数増

（３） 上位互換性要件

選定したソフトウェアについては、バージョンアッププランを考慮すること。

（４） システム中立性要件

サーバ機器等は、市場で一般的に販売されているものを選択すること。

（５） 事業継続性要件

信頼性要件に加え、障害及び災害発生時の事業継続のためにはデータ復旧が必要となるため、速やかな復旧を考慮したハードウェア・ソフトウェア構成、保守体制とすること。サーバ機器等は、市場で一般的に販売されているものを選択すること。

6. 情報セキュリティ要件

（１） 情報セキュリティ対策

受注者は、機構と調整の上、必要な対策を講じること。具体的には、別紙 2「セキュリティ対応方針と役割分担」を満たす製品、サービスを選定すること。

7. 情報システム稼動環境

（1） 全体構成

本システムの全体構成図を下図に示す。

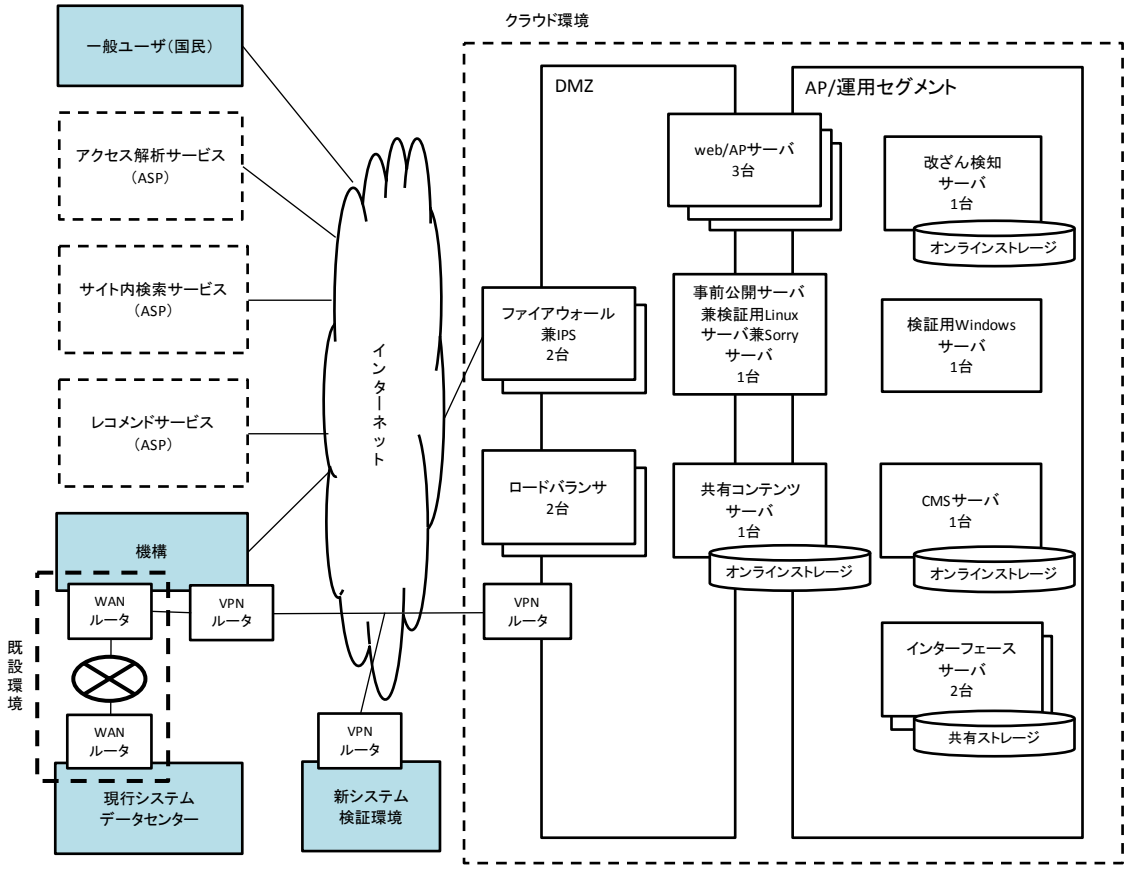


図 1　全体構成図

（2） ハードウェア・ソフトウェア構成

① サーバ台数

クラウド環境のハードウェア台数を下表に示す。

表 6　サーバ台数

項番	機器名称	台数	概要
1	Web/AP サーバ	3 台	Web サイトのコンテンツを公開するサーバ及び添付文書等検索に関するアプリケーションが稼働するサーバ また、外部 ASP サービスと連携する機能を有する
2	共有コンテンツサーバ	1 台	静的コンテンツ及び PDF ファイル等を格納するサーバ
3	インタフェースサーバ	2 台	現行システムデータセンター内の現行システムと連携し必要となるデータの受渡しを行うサーバ（Active-Stanby 冗長構成）

項番	機器名称	台数	概要
4	改ざん検知サーバ	1台	CMSサーバとWeb/APサーバとの間に介在し、Web/APサーバ上のコンテンツが改ざんされていないかを監視するサーバ
5	CMSサーバ	1台	Webサイトのコンテンツを作成、公開するためのサーバ
6	事前公開サーバ兼検証用 Linuxサーバ兼Sorryサーバ	1台	コンテンツを公開サーバ（Web/APサーバ）に公開する前にインターネット経由で事前に確認するためのサーバであり、かつ、セキュリティパッチ等を本番サーバに適用する前に事前に検証するためのLinuxサーバ。インターネットからのアクセスは厚生労働省からのみに制限する必要がある。また全Web/APサーバが停止した場合に利用者にシステム停止中であることを提示するSorryサーバも兼ねる。
7	検証用Windowsサーバ	1台	セキュリティパッチ等を本番サーバに適用する前に事前に検証するためのWindowsサーバ
8	オンラインストレージ	4台	共有コンテンツサーバ、改ざん検知サーバに各1ずつ、CMSサーバに2台使用する追加ストレージ
9	共有ストレージ	1台	インタフェースサーバ2台間で共有する高性能ストレージ
10	ファイアウォール兼IPS	2台	インターネットからのアクセス制御し不要なアクセスを防御するファイアウォール アクティブ・スタンバイの冗長構成。併せて不正侵入を検知するIPS機能も有する。
11	ロードバランサ	2台	インターネットからのWEBアクセスを複数台のWEB/APサーバに振り分ける負荷分散装置機能 アクティブ・スタンバイの冗長構成。 SSLサーバ証明書を搭載する[注1]
12	VPN接続用ルータ＃1	2台	クラウドセンター～機構間の拠点間VPN接続を行うためのルータ
13	VPN接続用ルータ＃2	1台	新システム検証環境～クラウドセンター及び機構間の拠点間VPN接続を行うためのルータ

[注1]サーバ証明書はEV SSL証明書を運用期間中利用可能となるものの導入を想定。

② 詳細仕様

本調達において必要となるハードウェア・ソフトウェア及び提供すべき外部 ASP サービスの詳細仕様を以下に示す。

表 7 ハードウェア仕様

項番	機器等名称	仮想 CPU ※1	仮想 MEM (GB)	仮想 HDD (GB)	仮想 NIC (GbE)
1	Web/AP サーバ	4	8	50	2
2	共有コンテンツサーバ	4	8	50	2
3	インタフェースサーバ	8	16	50	2
4	改ざん検知サーバ	2	4	50	2
5	CMS サーバ	4	8	50	2
6	事前公開サーバ兼検証用 Linux サーバ兼 Sorry サーバ	2	4	50	2
7	検証用 Windows サーバ	2	4	50	2

※1 64bit、1.25GHz 相当（CPU リソースは左記スペック以上を保証すること）

表 8 ストレージ構成

項番	機器等名称	サイズ (GB)	備考
1	共有コンテンツ用ストレージ	1000	RAID1 構成、実使用量記載、10,000IOPS
2	改ざん検知用ストレージ	1000	RAID1 構成、実使用量記載、10,000IOPS
3	CMS 用ストレージ#1	1000	RAID1 構成、実使用量記載、10,000IOPS
4	CMS 用ストレージ#2	1000	RAID1 構成、実使用量記載、10,000IOPS
5	インタフェース用ストレージ	3000	RAID5 構成、実使用量記載、20,000IOPS

表 9　ソフトウェア仕様

項番	機器等名称	OS ※1	OS ※2	WEB・APサーバ	全文検索エンジン	ファイル共有	コンテンツ管理 ※3	改ざん検知 ※4	データベース ※5	ウィルス対策 ※6	運用監視 ※7	JAVA実行環境	メール送信 ※8	SSL証明書 ※9	クラスタソフト
1	Web/APサーバ	－	○	○	－	－	－	－	－	○	○	○	－	○	－
2	共有コンテンツサーバ	－	○	－	－	○	－	－	－	○	○	－	－	－	－
3	インタフェースサーバ	－	○	－	○	－	－	－	○	○	○	○	－	－	○
4	改ざん検知サーバ	○	－	－	－	－	－	○	－	○	○	－	－	－	－
5	CMSサーバ	－	○	－	－	－	○	－	－	○	○	○	○	－	－
6	事前公開サーバ兼検証用 Linuxサーバ兼Sooryサーバ	－	○	○	－	－	－	－	－	○	○	○	－	○	－
7	検証用 Windowsサーバ	○	－	－	－	－	－	○	－	○	○	－	－	－	－
8	オンラインストレージ	－	－	－	－	－	－	－	－	－	○	－	－	－	－
9	共有ストレージ	－	－	－	－	－	－	－	－	－	○	－	－	－	－

※1　Microsoft Windows 2008 R2。但しクラウドサービス提供のVPSにてライセンス提供を含む場合は不要。別途ソフトウェアの導入が必要な場合は導入作業、インストールメディア・マニュアル納品、利用期間ライセンス費用、保守費用を含む。

※2　RedHat Enterprise Linux 6。但しクラウドサービス提供のVPSにてライセンス提供を含む場合は不要。別途ソフトウェアの導入が必要な場合は導入作業、インストールメディア・マニュアル納品、利用期間ライセンス費用、保守費用を含む

※3　ALAYA。インストールメディア・マニュアル納品、利用期間ライセンス費用、保守費用を含む。(別紙「医薬品医療機器情報提供システム　HW／SW基本設計書」を参照のこと)

※4　別紙「医薬品医療機器情報提供システム　HW／SW基本設計書」に記載の要件を満たすソフトウェアのインストールメディア・マニュアル納品、利用期間ライセンス費用、保守費用を含む。

※5　Oracle 11g Standard Edition ONE。インストールメディア・マニュアル納品、利用期間ライセンス費用、保守費用を含む。
[注]仮想化稼働環境において必要となるライセンスについて提供すること。

※6　Trendmicro ServerProtect for Linux / Trendmicro Server Protection for Windows

相当。リアルタイムスキャンが可能であること。但しクラウドサービスとして同等の機能の提供が可能な場合は不要。別途ソフトウェアの導入が必要な場合は導入作業、インストールメディア・マニュアル納品、利用期間ライセンス費用、保守費用を含む。

※7　別紙 4「運用監視・保守方針と役割分担」を満たすクラウドサービス機能として想定利用期間の間提供すること。サービス提供でない場合は、本件受注者が自己の責任と負担において導入作業期間内に導入・設定作業を実施すること。併せてインストールメディア・マニュアル納品、利用期間ライセンス費用、保守費用を含む。

※8　CMS から機構職員への通知メール及び運用監視通知メール用

※9　Web/AP サーバには SSL 通信を実現するためのサーバ証明書を必要台数分提供すること。平成 26 年 7 月 1 日～平成 31 年 3 月 31 日の期間、利用可能な証明書を提供すること。サーバ証明書は EV SSL 証明書であること。

表 10　外部 ASP サービス仕様

項番	サービス名称	サービス概要
1	サイト内検索サービス	別紙「医薬品医療機器情報提供システム　HW／ＳW基本設計書」に示す要件を満たす外部サービスを想定利用期間の間提供すること
2	アクセスログ解析サービス	
3	レコメンドサービス	

（3）　ネットワーク構成

① ネットワーク個別要件

ア．クラウドセンター内 LAN 要件

- 回線速度は 1Gbps 以上とする。
- バックアップ等の大容量転送時にも性能低下が発生しないように、十分なパケット処理能力を確保すること。
- ネットワークセグメントはフロントネットワークセグメント（DMZ）、運要管理セグメントを想定している。必要に応じて外部インタフェース用セグメントを分離する可能性がある。設計に応じて VLAN 設定が行えること。

イ．インターネット接続要件

クラウドセンターとインターネットサービスプロバイダ（以下「ISP」という。）間の接続は、次に示す回線容量と帯域保証を実現すること。またマルチキャリアで冗長化されたインターネット接続環境を提供すること。

表 11　インターネット回線

項番	接続拠点	回線容量・帯域保証
1	クラウドセンター	100Mbps ベストエフォート（※1）

（※1）ベストエフォート型とは、帯域保証のない通信サービスのこと。

クラウドセンターにて用意するインターネット接続回線の要件は以下のとおりとする。

- 本システム利用者が、インターネットを介して本システムにアクセスできるインターネット接続環境を提供できること。
- インターネット接続回線はギガビット対応回線であること。

ウ．外部接続（VPN 接続）要件

クラウドセンターのサービスで専用の外部接続を行う場合は、必要な回線を敷設すること。インターネット接続回線を利用した VPN 接続サービスの場合は、「４．規模・性能要件」を満たすことを前提にユーザからのアクセスに影響が出ない構成を提案すること。また経路は暗号化されているものを提供すること。さらに運用作業時に使用するリモートアクセス用 SSL-VPN 接続サービスを 2 ユーザ分提供すること。リモートアクセス用 SSL-VPN 接続サービスはユーザ ID/パスワード認証にワンタイムパスワード認証を追加した 2 要素認証機能を提供し、セキュアなリモートアクセス環境を実現すること。

なお、VPN 回線の要件は以下のとおりとする。

- 接続する拠点は将来的に増減することが容易であること。
- 回線網は、次に示す回線容量と帯域保証を実現すること。

表 12　VPN 回線

項番	接続拠点	回線容量・帯域保証
1	クラウドセンター～機構間 及び新システム検証環境	100Mbps ベストエフォート（※1）

（※1）ベストエフォート型とは、帯域保証のない通信サービスのこと。

エ．クラウドセンター～現行データセンター間

クラウドセンターと現行データセンター間は機構をブリッジ経由し接続することとする。

オ．グローバル IP アドレス要件

- クラウド環境提供事業者は、本システムに必要となるグローバル IP アドレスを 4 個提供すること。

② ネットワーク機器構成

表 13　クラウドセンター用ネットワーク機器

項番	機器名称	台数	備考
1	ファイアウォール	2 台	1 台はバックアップ
2	ロードバランサ	2 台	1 台はバックアップ
3	VPN 接続用ルータ兼ファイアウォール	1 台	クラウドセンター～機構

※上記機器については、クラウドサービスとして提供可能なものはサービス提供形態とする。別途クラウドセンター内に持ち込み等必要な場合は、本件受注者にてクラウドセンター内への機器納入、設置を行うこと。

表 14　機構及び新システム検証環境用ネットワーク機器

項番	機器名称	台数	備考
1	VPN 接続用ルータ兼ファイアウォール	1 台	クラウドセンター～機構

項番	機器名称	台数	備考
2	VPN 接続用ルータ兼ファイアウォール	1 台	新システム検証環境～機構及びクラウドセンター

③　ネットワーク機器共通要件

ア．ICMP による死活監視が可能なこと

イ．SNMP による管理が可能なこと

ウ．Syslog 管理サーバにログを転送する機能を有すること

④　ネットワーク機器個別要件

各ネットワーク機器は下表の要件を満たすこと

表 15　ネットワーク機器個別要件

項番	機器名称	区分	備考
1	ファイアウォール兼 IPS	フィルタリング機能	ルールに基づき通信の許可/拒否の処理を行う
		対応プロトコル	IP、ICMP、TCP、UDP、ESP、AH、GRE
		送信元/宛先 IP アドレス	特定アドレス、サブネットマスク、グループ
		アドレス変換（NAT）	双方向 1 対 1 の NAT、双方向 1 対 N の NAPT、片方向 1 対 N の NAPT
		分割	ファイアウォールはインスタンス単位で分割可能であること
		IP アドレス	インターネット VPN で接続する際に NAT 変換を不要とするため IP アドレスの持込みが可能であること
2	ロードバランサ	処理能力	200Mbps ベストエフォート
		対応プロトコル	レイヤ 4
		分散アルゴリズム	ラウンドロビン、最小コネクション（リーストコネクション）、送信元 IP アドレスハッシュ、URL ハッシュ
		セッション維持	送信元 IP アドレス、Cookie（ロードバランサ）、Cookie（サーバ）、URL、SSL セッション ID

項番	機器名称	区分	備考
		ヘルスチェック	ICMP（IP レベルチェック）、TCP（ポートレベルチェック）、 HTTP（リクエストのチェック）
		SSL 暗号化	サーバ、ロードバランサ間の SSL 暗号化
		Sorry サーバ	分散対象サーバのヘルスチェックが確認できない場合に決められた Sorry サーバに通信を割り振る
3	VPN 接続用ルータ	インタフェース	10/100/1000BASE-T×2
		ルーティングプロトコル	RIP、RIP2、OSPF、BGP4(EBGP、IBGP)等
		カプセル化	VLAN、PPP、フレームリレー、PPPoE、MP
		トラフィック管理	QoS、重み付けランダム早期検出、階層型 QoS
		セキュリティ	組み込みハードウェア暗号化アクセラレーション、VPN サービス（IPSec と SSL アクセラレーションの両方）
4	リモートアクセス用 SSL-VPN （必要数：2）	利用単位	ユーザ環境毎に一式
		アクセス経路	インターネット経由
		帯域	ベストエフォート
		通信ポート制限	なし
		認証方式	2 要素認証（ユーザ ID/パスワード認証＋ワンタイムパスワード認証）
		ワンタイムパスワードトークン	ソフトウェアトークン

（4） アクセシビリティ要件

なし。

（5） クラウド要件

クラウドの要件について以下のとおり定義する。

① クラウド方式の定義

ア. IaaS（Infrastructure as a Service）上の VPS を用いたパブリッククラウドを想定している。インターネット経由のアプリケーション実行用プラットフ

ォーム及びストレージを提供すること。

イ．必要にあわせてサーバやストレージを利用可能なこと。

ウ．様々なプラットフォームからネットワークを通じ利用できること。

② クラウド全体構成要件

ア．サービス提供時間

計画停止時間を除き、24 時間、年中無休でサービス提供を行うこと。なお、ユーザ側の要望がある場合、可能な限り計画停止タイミングについて調整可能であること。

イ．可用性

稼働率 99.99%を実現可能な構成とすること。また、サービス単位でサービスレベルが定義でき、レベルを選択可能であること。

ウ．バックアップ・リカバリ

別紙 3「バックアップ・リカバリ方針」に示す事項を満たすサービス提供を行うこと。

エ．拡張性

サーバ、ストレージのリソースはシステムを再構築することなく割当て変更可能であること。

オ．信頼性

- サーバが停止した場合に一般ユーザに影響が発生する機能を担うサーバは、2 台以上の冗長構成とし、片系のサーバでの障害発生又は OS の停止を行っても業務を継続できる構成とする。
- 性能が低下することで一般ユーザに影響が発生する機能を担うサーバは、性能要件を満たすために必要なサーバ台数に 1 台追加した構成をとることで、サーバ 1 台で障害が発生した場合にも性能要件を満たす冗長構成とする。
- サーバが停止しても一般ユーザへの影響が発生しない運用管理機能を担うサーバは、原則 1 台構成とする。ただし運用上必要なデータについては適宜バックアップを取得し、サーバ復旧後速やかにバックアップから復旧を行うこととする。
- 仮想サーバを搭載する物理サーバは原則、サーバの全てのコンポーネントを冗長化（電源ユニットの 2 重化、FAN の 2 重化、内蔵ディスクのミラー化、NIC の 2 重化など）することでサーバ単体の耐障害性を高めることとする。ただし、ブレード型サーバなどで I/F カードの冗長化が難しい場合は port レベルでの冗長化とする。
- 物理サーバ障害やメンテナンス時でも動的に仮想サーバを切り替えることでシステム稼働への影響を少なくすることが可能であること
- 標準で仮想サーバに対する HA(High Availability)機能を提供できること

カ．仮想化ソフト

「ソフトウェア構成」で指定するソフトウェアがサポートされる仮想化ソフトを使用すること。

キ．セキュリティ

本システムの扱うデータのセキュリティレベルを鑑み、クラウド環境は以下の事項を満たすこと。

- 仮想化ソフトの管理者権限ユーザを確実に管理すること。
- ISMS 認証（ISO27001）を取得し情報セキュリティ外部監査を受けていること
- セキュリティ・インシデント／イベントへの対応をしていること
- 顧客間のリソース分割は VLAN レベルでの分離ではなく、専用の仮想ファイアウォールによる完全分離された構成とすること
- クラウド環境内のセキュリティアップデートを管理する WSUS/yum サーバにより必要なモジュールの適用が可能なこと

ク．管理機能（ポータルツール）

以下について管理可能なポータル機能を日本語で提供すること

- アカウント管理（利用ユーザ作成、変更、削除）
- 仮想サーバ管理（作成、変更、削除、電源 ON/OFF、バックアップ等）
- ネットワーク管理（IP アドレス取得等）
- ファイアウォール管理（ACL、アドレスグループ、NAT 等）
- ロードバランサ管理（負荷分散、SSL 証明書等）
- システム監視状況閲覧
- サービスデスク（IaaS 監視、障害対応）

ケ．時刻同期（NTP）

クラウド環境内の NTP サーバにより時刻同期が可能なこと

（６） クラウドセンター施設設備要件

① 施設建築物に関する要件

ア．データセンター専用の建物又は準じた対応が施されていること。

イ．クラウドセンターの所在地は日本国内に設置されていること。

ウ．震度 7 の地震に耐える耐震又は免震構造で建築されていること。

エ．日本データセンター協議会（JDCC）が定義するファシリティスタンダードで「Tier3」以上であること。

オ．予想最大損失率 PML（Probable Maximum Loss）値が 5%未満であること。

カ．建築物総合環境性能評価システム CASBEE(Comprehensive Assessment System for Building Environment Efficiency)が「S ランク」であること。

② 立地要件

ア．地震、風水害、塩害及び落雷等、自然災害の影響の少ない場所に立地していること。(国土交通省・各自治体が公開しているハザードマップにて危険性の指摘がない、文部科学省が示す主要活断層帯を避けた場所であること等)

③　設備要件

ア．電源設備に関する要件

- 電力供給は、災害時等においても無停電電源装置（UPS 設備）、自家発電設備により途切れることなく 24 時間 365 日安定供給すること。なお、無停電電源装置（UPS 設備）の冗長化を実現できる建物であること。自家発電設備は無給油で 72 時間以上の連続稼働を行えること。なお、途中給油によって更にそれ以上の連続稼働を行えること。
- 停電等により通常の電力供給が停止した場合、自家発電装置による電力供給を行うまでの間は、UPS 設備によりサーバ機器設置室等必要な箇所に無瞬断で電力を供給できること。なお、将来の信頼性向上の要求に応えられるよう、自家発電電装の冗長化を実現できる建物であること。また、電力供給は 2 か所の変電所から電源供給を受けられること。
- 電力設備の定期点検等を行う場合も無停止で電力供給が可能であること。
- CVCF（定電圧定周波電源装置）を通して電力供給すること。
- PUE（Power Usage　Effectiveness）値は、「1.5 以下」であること。

イ．空調設備に関する要件

- 不具合や障害発生時（災害時等の商用電源停止時等）、点検実施時に影響なく、納入する機器類が正常稼動できる温度（5～35℃）、湿度（20～80%、但し結露しないこと）を 24 時間 365 日維持できること
- 空調効率向上のため、ラックの前面がコールドアイル、裏面がホットアイルとなるレイアウトとし、かつアイルキャッピング等によりホットアイルの暖気をコールドアイルの冷気と分離する等の仕組みを講じること。

ウ．消火設備に関する要件

- 建築基準法、消防法に基づいた耐火建築物であり、火災報知システムを有していること。
- 隣接建物からの延焼防止装置が施されていること。また、火災発生時の消火活動に必要となる消火器、消火栓が設置されていること。
- 建築基準法施行令に規定する排煙設備が建物内の適切な個所に設置されていること。

エ．セキュリティに関する要件

- サーバルームへの入退室は、電子錠によりロックされており、生体認証又はカード認証により個人を特定し、ロックを開錠し、入退室ができること。また、共連れ防止機能を備えていること。
- サーバルームの入退室は、監視カメラにより 24 時間 365 日監視すること。
- サーバルームへの入退室の記録は、ログとして保存されていること。
- 建物への入館は、有人による 24 時間 365 日の運用、監視を実施すること。
- データセンターの建物内への入館管理、サーバルームへの入館管理、ラッ

ク開閉管理を行うこと。

- データセンターの入館者に対し機構担当職員からの申請により作業立会いの依頼があった場合は、機構担当職員に代わり作業立会いを実施すること。
- 緊急時の入館ルールが明確化されており、当日等の緊急入館ができること。

（７） 運用監視・保守要件

クラウドセンターは、別紙 4「運用監視・保守方針と役割分担」に示す運用サービス及び監視サービスを有し、運用・監視対応可能な状態でのクラウド環境提供が可能なこと。

8. 作業の体制及び方法

（１） 作業体制

受注者は、業務受託後、機構に対して作業体制（受注者側の体制図とそれぞれの役割の詳細）を報告し、承認を得て業務を進めること。この際、業務に従事する者のスキル（「IT スキル標準（ITSS)」）や資格、これまでの業務実績を明記すること。

なお、作業体制には PM（プロジェクト・マネージャー）を設置すること。

（２） 瑕疵担保責任

本業務の瑕疵担保責任の範囲・期間等の瑕疵への対応については、契約に基づき規定するものとする。

受注者は、瑕疵担保責任を果たす上で必要な情報を整理し、その一覧を機構に提出すること。瑕疵担保責任の期間が終了するまで、それら情報が漏洩しないように、ISO/IEC27001認証（国際標準）又はJISQ27001 認証（日本工業標準）に従い、厳重に管理をすること。

また、瑕疵担保責任の期間が終了した後は、速やかにそれら情報についてデータ復元ソフトウェア等を利用してもデータが復元されないように完全に消去すること。データ消去作業終了後、受注者は消去完了を明記した証明書を作業ログとともに機構に対して提出すること。なお、データ消去作業に必要な機器等については、受注者の負担で用意すること。

9. 特記事項

（１） 基本事項

受注者は、次に掲げる事項を遵守すること。

① 本業務の遂行に当たり、業務の継続を第一に考え、善良な管理者の注意義務をもって誠実に行うこと。
② 本業務に従事する要員は、機構と円滑なコミュニケーションを行う能力と意思を有していること。
③ 本業務の履行場所を他の目的のために使用しないこと。
④ 本業務に従事する要員は、履行場所での所定の名札の着用等、従事に関する所定の規則に従うこと。
⑤ 要員の資質、規律保持、風紀及び衛生・健康に関すること等の人事管理並びに要員の

責めに起因して発生した火災・盗難等不祥事が発生した場合の一切の責任を負うこと。

⑥ 受注者は、本業務の履行に際し、機構からの質問、検査及び資料の提示等の指示に応じること。また、修正及び改善要求があった場合には、別途協議の場を設けて対応すること。

⑦ 次回の本業務調達に向けた現状調査、機構が依頼する技術的支援に対する回答、助言を行うこと。

（２） 入札制限

情報システムの調達の公平性を確保するために、以下に示す事業者は本調達に参加できない。

① 機構 CIO 補佐が現に属する、又は過去 2 年間に属していた事業者等

② 各工程の調達仕様書の作成に直接関与した事業者等

③ 設計・開発等の工程管理支援業者等

④ ①～③の親会社及び子会社（「財務諸表等の用語、様式及び作成方法に関する規則」（昭和 38 年大蔵省令第 59 号）第 8 条に規定する親会社及び子会社をいう。以下同じ。）

⑤ ①～③と同一の親会社を持つ事業者

⑥ ①～③から委託を受けるなど緊密な利害関係を有する事業者

（３） 応札条件

応札希望者は、以下の資格等を満たしていること。

① 開発責任部署は ISO9001 又は CMMI レベル 3 以上の認定を取得していること。

② ISO/IEC27001 認証（国際標準）又は JISQ27001 認証（日本工業標準）のいずれかを取得していること。

③ プライバシーマーク付与認定を取得していること。

④ PM（プロジェクト・マネージャー）は特定非営利活動法人日本プロジェクトマネジメント協会の「プロジェクトマネジメント・スペシャリスト（PMS)」、PMI （Project Management Institute）の「PMP」資格、独立行政法人情報処理推進機構（IPA）の「プロジェクトマネージャ」資格のいずれかを取得していること。

⑤ 公示後設定された期間に設計書等を閲覧した記録があること。あるいは過去の案件において設計書等を閲覧したことを証明する記録があること。

⑥ 提供するクラウド環境は、中央官庁又は独立行政法人の保有するシステムを稼動させた実績を保有すること。併せて本システム同様、高セキュリティを必要とする医療関連システムの稼動実績を保有すること。

⑦ 本調達仕様書で示した機材・サービスの一切を提供可能であることを証する書類一式を入札前に提出すること。

（４） 知的財産等

知的財産の帰属は、以下のとおり。

① 本件に係り作成・変更・更新されるドキュメント類及びプログラムの著作権（著作権法第 21 条から第 28 条に定めるすべての権利を含む。）は、受注者が本件のシステ

ム開発の従前より権利を保有していた等の明確な理由により、あらかじめ書面にて権利譲渡不可能と示されたもの以外、機構が所有する等現有資産を移行等して発生した権利を含めてすべて機構に帰属するものとする。

② 本件に係り発生した権利については、受注者は著作者人格権（著作権法第 18 条から第 20 条までに規定する権利をいう。）を行使しないものとする。

③ 本件に係り発生した権利については、今後、二次的著作物が作成された場合等であっても、受注者は原著作物の著作権者としての権利を行使しないものとする。

④ 本件に係り作成・変更・修正されるドキュメント類及びプログラム等に第三者が権利を有する著作物が含まれる場合、受注者は当該著作物の使用に必要な費用負担や使用許諾契約に係る一切の手続きを行うこと。この場合は事前に機構に報告し、承認を得ること。

⑤ 本件に係り第三者との間に著作権に係る権利侵害の紛争が生じた場合には、当該紛争の原因が専ら機構の責めに帰す場合を除き、受注者の責任、負担において一切を処理すること。この場合、機構は係る紛争の事実を知ったときは、受注者に通知し、必要な範囲で訴訟上の防衛を受注者にゆだねる等の協力措置を講ずる。

⑥ なお、受注者の著作又は一般に公開されている著作について、引用する場合は出典を明示するとともに、受注者の責任において著作者等の承認を得るものとし、機構に提出する際は、その旨併せて報告するものとする。

（５） 再委託

受注者は、受注業務の全部又は主要部分を第三者に再委託することはできない。なお、本業務における主要部分とは、クラウド環境提供、プロジェクト管理作業を想定している。受注業務の一部を再委託する場合は、事前に再委託する業務、再委託先等を機構に申請し、承認を受けること。申請にあたっては、「再委託に関する承認申請書」の書面を作成の上、受注者と再委託先との委託契約書の写し及び委託要領等の写しを機構に提出すること。

受注者は、機密保持、知的財産権等に関して本仕様書が定める受注者の責務を再委託先業者も負うよう、必要な処置を実施し、機構に報告し承認を受けること。

なお、第三者に再委託する場合は、その最終的な責任を受注者が負うこと。特に本調達内の要求機能においては外部ASPサービスの利用を想定しているものが存在するが、それらも含め全ての最終的な責任を受注者が負うこと。

（６） 機密保持

本業務を実施する上で必要とされる機密保持に係る条件は、以下のとおり。

① 受注者は、受注業務の実施の過程で機構が開示した情報（公知の情報を除く。以下同じ。）、他の受注者が提示した情報及び受注者が作成した情報を、本受注業務の目的以外に使用又は第三者に開示若しくは漏洩してはならないものとし、そのために必要な措置を講じ、瑕疵担保責任の期間が終了するまで、それら情報が漏洩しないように、ISO/IEC27001 認証（国際標準）又は JISQ27001 認証（日本工業標準）に従い、厳重に管理をすること。また、瑕疵担保責任を果たす上で必要な情報については、瑕疵担保責任の期間が終了するまで、同様に管理すること。

② 受注者は、本受注業務を実施するにあたり、機構から入手した資料等については管理

台帳等により適切に管理し、かつ、以下の事項に従うこと。

- 複製しないこと。
- 用務に必要がなくなり次第、速やかに機構に返却又は消去すること。
- 受注業務完了後、上記①に記載される情報を削除又は返却し、受注者において該当情報を保持しないことを誓約する旨の書類を機構に提出すること。

③ 「秘密保持等に関する誓約書」を別途提出し、これを遵守しなければならない。

④ 応札希望者についても上記①及び②に準ずること。

⑤ 「独立行政法人医薬品医療機器総合機構 情報システム管理利用規程」の第 52 条に従うこと。

⑥ 機密保持の期間は、当該情報が公知の情報になるまでの期間とする。

（７） 遵守事項

本業務を実施するにあたっての遵守事項は、以下のとおり。

① 受注者は、「政府機関の情報セキュリティ対策のための統一基準（第 4 版）」（平成 21 年 2 月 3 日、情報セキュリティ政策会議決定）に定めるほか、機構が定める情報セキュリティの規定を遵守すること。またそれら各規定の改訂状況についても注視をし、常に最新の規定を遵守するよう努めること。

② 機構へ提示する電子ファイルは事前にウイルスチェック等を行い、悪意のあるソフトウェア等が混入していないことを確認すること。

③ 民法、刑法、著作権法、不正アクセス禁止法、個人情報保護法等の関連法規を遵守することはもとより、下記の機構内規程を遵守すること。

- 独立行政法人 医薬品医療機器総合機構 情報システム管理利用規程

④ 独立行政法人 医薬品医療機器総合機構 個人情報管理規程受注者は、本業務において取り扱う情報の漏洩、改ざん、滅失等が発生することを防止する観点から、情報の適正な保護・管理対策を実施するとともに、これらの実施状況について、機構が定期又は不定期の検査を行う場合においてこれに応じること。万一、情報の漏洩、改ざん、滅失等が発生した場合に実施すべき事項及び手順等を明確にするとともに、事前に機構に提出すること。また、そのような事態が発生した場合は、機構に報告するとともに、当該手順等に基づき可及的速やかに修復すること。

（８） 作業場所

受注業務の作業場所は、（再委託等も含めて）機構内、又は日本国内で機構の承認した場所で作業すること。機構内での作業においては、必要な規定の手続を実施し承認を得ること。

なお、必要に応じて機構職員は現地確認を実施できることとする。

（９） 環境への配慮

環境への負荷を低減するため、以下に準拠すること。

① 本件に係る納入成果物については、「国等による環境物品等の調達の推進等に関する法律（グリーン購入法）」（平成 15 年 7 月 16 日法律第 119 号）に基づいた製品を可能な限り導入すること。

② 導入する機器等がある場合は、性能や機能の低下を招かない範囲で、消費電力節減、発熱対策、騒音対策等の環境配慮を行うこと。

（１０）　　その他

機構全体管理組織（PMO）が担当課に対して指導、助言等を行った場合には、受注者もその方針に従うこと。

10. 留意事項

① 本提案に要する費用は、提案者の負担とする。
② 本業務を遂行するために機構に対する資料要求、要望等がある場合は、原則文書にて行うこと。
③ 本業務を実施するにあたり必要な情報は、機構と受注者との間で秘密保持に関する契約を行うこととする。
④ 本業務を遂行する上で、機構の役職員等へのヒアリングが必要な場合は、必用最小限に留め、効率よく実施すること。
⑤ 本仕様書に掲げられている事項の他、本業務を遂行するために必用な事項は機構担当者と協議の上、実施すること。
⑥ 本業務における提出物等の公表にあたっては、支援業者名も併せて公表することとする。
⑦ 本業務を遂行する上で発生した書面（電子媒体を含む。）、その他類似の派生物（企画等の構想も含む。）は、一切の著作権、所有権及び使用権を機構に帰属するものとする。また、成果物の著作人格権は行使しないことを契約書にて締結することとする。
⑧ 機能証明書提出時に、機構又は機構以外の国、地方公共団体、独立行政法人における規制当局で本調達に類する業務を請け負った実績について提出すること。
⑨ 応札にあたっては、必ず入札説明会に参加した上で、最低限、以下の書類の内容を熟知しておくこととする。

- 総合機構パンフレット
- 独立行政法人医薬品医療機器総合機構法
- 独立行政法人医薬品医療機器総合機構審査等業務及び安全対策業務関係業務方法書
- 独立行政法人医薬品医療機器総合機構 救済業務関係業務方法書
- 独立行政法人医薬品医療機器総合機構平成２０事業年度業務報告
- 独立行政法人医薬品医療機器総合機構平成２１事業年度業務報告
- 独立行政法人医薬品医療機器総合機構平成２２事業年度業務報告
- 独立行政法人医薬品医療機器総合機構平成２３事業年度業務報告
- 独立行政法人医薬品医療機器総合機構平成２４事業年度業務報告
- 独立行政法人医薬品医療機器総合機構業務・システム最適化計画

※上記については総合機構ホームページに掲載されている。

11. 窓口連絡先

独立行政法人 医薬品医療機器総合機構 情報化統括推進室
電話：03－3506－9485

以上

別紙１：　セキュリティ脆弱性診断要件

本調達における脆弱性診断とは当該システムに「その時点での脆弱性が存在するか」を調査することである。OS、ミドルウェア、DBMS、あるいは当該システム上で稼働しているWebアプリケーションは、リリースされてから使用される期間が長くなればなるほど脆弱性が発見される可能性が高くなり、結果的に、長く使用しているシステム程、脆弱性を内包している危険性が高まる。また、新しい攻撃手法については、当初は開発した攻撃者だけが使用しているため、攻撃対象は限定的であるが、時間を経てその攻撃手法がインターネット等を介して広まっていくとマルウェア化され、被害は加速度的に広がっていく。また、機構のセキュリティ対策の質的向上を期すため、各年度毎に脆弱性及び対策状況の推移を示すことが求められており、期間中、診断項目や精度は、高いレベルで同一に維持される必要がある。
以下に期間中に実施すべきセキュリティ診断要件を示す。

基本要件

- プラットフォーム診断は、診断の網羅性及び正確性を担保するために、1 種類の商用診断ツールのみで行うのではなく、目的に応じた複数の診断ツールを併用し、かつ診断担当者による手動診断を実施すること。
- Web アプリケーション診断は、診断の網羅性及び正確性を担保するために、担当者による手動診断で実施すること。やむを得ず商用診断ツールを使用する場合には、ツール適用範囲は50%以下とすること。
- 診断にあたっては、事前に診断対象、診断内容、診断スケジュール、診断担当者、緊急時連絡方法等を記載した、診断内容確認書を作成すること。
- 作業時間は、原則平日 10:00～17:00 とするが、必要に応じて夜間・深夜・休日等にも対応すること。
- 診断中に緊急度の高い脆弱性が発見された場合、報告会や報告書作成を待たずして対策を実施するために、問題点とその原因（詳細記述）、脅威の内容、緊急性、考えられる被害、具体的な対応策、関連情報、リスク対策等を記載した速報を診断日の翌営業日までに提出すること。
- 契約期間中、年度毎に検知された脆弱性の数や種類を比較・分析し、年次で報告すること。
- 検出された脆弱性に対して、効果的な対策を提案し、提供できる部門を有すること。
- 診断業務の品質を担保するために、脆弱性診断を担当する部門に置いて ISO9001 の認証を取得していること。また、本件における品質管理体制と役割を示すこと。
- 機構のセキュリティ情報を取り扱うため、診断を実施する当該部門、又は全社で ISMS の認証を取得していること。
- プラットフォーム診断について、リモート診断及びオンサイト診断と合わせて、年間 1000 IP 以上の診断実績を、直近の 5 年以上継続していること。これを客観的に証明できる証憑を提示すること。
- Web アプリケーション診断について、1000 画面遷移以上の診断実績を、直近の 5 年以上継続していること。これを客観的に証明できる証憑を提示すること。
- 診断にあたっては、責任者と実施担当者で構成される診断チームを編成すること。
- 診断チームの責任者は 10 年以上の診断実績を有し、機構との会合に下記いずれか

の資格を有する者が参画すること。

- ✧ 公認システム監査人
- ✧ 公認情報システム監査人（CISA）
- ✧ 公認情報システムセキュリティ専門家（CISSP）
- ✧ 情報セキュリティスペシャリスト

● 診断の実施担当者は、診断経験 3 年以上で、下記いずれかの資格を有する者で構成されること。

- ✧ 公認システム監査人
- ✧ 公認情報システム監査人（CISA）
- ✧ 公認情報システムセキュリティ専門家（CISSP）
- ✧ 情報セキュリティスペシャリスト
- ✧ テクニカルエンジニア（ネットワーク）

別紙２：　セキュリティ対応方針と役割分担

対策区分	対策方針	対策要件	目的	対応方針	実施者		
					受注者	設計・開発業者	運用・保守業者
侵害対策	通信回線対策	通信経路の分離	不正行為の影響範囲を限定的にするため、業務に応じて通信経路（ネットワーク）の分離を行うこと。	FW サーバ又はサービスを提供する	○	-	-
				FW の設定を行う	-	○	-
				VLAN で DMZ による外部アクセス向けネットワークを分離可能なサービスを提供する	○	-	-
		不正通信の遮断	不正プログラムによる情報漏洩等の被害を防止するため、マルウェア感染防止の対策を行うこと。	ウィルス対策ソフト又はサービスを提供する	○	-	-
		通信のなりすまし防止	通信回線を介したなりすましによる不正を防止すること。	VPS 管理画面は特定の VPN 接続元以外からの通信を受付けないサービスを提供する	○	-	-
				インターネットからのユーザ向けサービスに SSL を使用する場合は信頼された証明書を導入する	○	-	-
				特定利用者にのみ提供するサービスの場合には、AP の認証方式を構築する	-	○	-
		サービス不能化の防止	トラフィック集中によるサービス不能化の脅威を軽減すること。	ロードバランササーバ又はサービスを提供する	○	-	-
				脆弱性をターゲットにした DoS 攻撃に対してはサーバに対する脆弱性対策（パッチ適用）を実施する	-	-	○
	不正プログラム対策	マルウェアの感染防止	不正プログラムによる情報漏洩等の被害を防止するため、マルウェア感染防止の対策を行うこと。	ウィルス対策ソフト又はサービスを提供する	○	-	-

対策区分	対策方針	対策要件	目的	対応方針	実施者		
					受注者	設計・開発業者	運用・保守業者
		マルウェア対策の管理	不正プログラム対策の最新化を確実に行うため、マルウェア対策状況を管理すること。	ウィルス対策ソフト又はサービスを提供する	○	-	-
	セキュリティホール対策	構築時の脆弱性対策	情報システムの脆弱性をついた攻撃を予め防ぐため、脆弱性の有無を確認し対処すること。	OS に対するパッチ適用サービスを提供する	○	-	-
				OS、ミドルウェアに対する脆弱性対策を実施する	-	○	-
				AP のセキュアコーディングを徹底する	-	○	-
				情報セキュリティに配慮したシステム設定を行う	-	○	-
				総合テスト前に外部セキュリティ診断を実施、報告する	-	○	-
		運用時の脆弱性対策	運用開始後に発見される脆弱性について、その改善を行うための対策を実施すること。	OS に対するパッチ適用サービスを提供する	○	-	-
				OS、ミドルウェアに対する脆弱性対策を実施する	-	-	○
				年 1 回外部セキュリティ診断を実施、報告する	-	-	○
不正監視・追跡	証跡管理	証跡の蓄積・管理	不正行為の検知、原因追求を行うため、情報システムのログの収集・蓄積・保管を行うこと。	FW ログ保管サービスを提供する	○	-	-
				OS、ミドルウェアのログを取得・保管する	-	-	○
		証跡の保護	不正な証跡の改変や削除を防止するため、証跡保護を行うこと。	FW ログへのアクセス可能なインタフェースは読み取り専用となるサービスを提供する	○	-	-
				OS、ミドルウェアのログに対するアクセス制御を実施する	-	○	-
		時刻の正確性確保	証跡の発生時刻を正確に把握することで正確な分析を行うため、システム全体の時刻を同期させること。	NTP サービスを提供する	○	-	-

対策区分	対策方針	対策要件	目的	対応方針	実施者		
					受注者	設計・開発業者	運用・保守業者
	不正監視	侵入検知	外部ネットワークから侵入による情報セキュリティの侵害を防止するため、不正侵入の検知を行うこと。	FW サーバ又はサービスを提供する	○	-	-
				FW の設定を行う	-	○	-
		サービス不能化の検知	トラフィック集中によるサービス不能化を検知すること。	FW のフロント側のトラフィック量を検知可能なサービスを提供する	○	-	-
アクセス・利用制限	主体認証	主体認証	許可されていない利用者のアクセスを防止するため、アクセス主体を認証するための機能を備えること。	VPS 管理用アクセスは SSL-VPN の二要素認証において制御可能なサービスを提供すること	○	-	-
				特定利用者にのみ提供するサービスの場合には、AP の認証方式を構築する	-	○	-
				パスワードの定期更新運用の実施	-	-	○
データ保護	機密性・完全性の確保	通信経路上の盗聴防止	通信経路上に流れるデータが盗聴された場合でも影響を低減させるための措置を行うこと。	VLAN で情報を保存する機器を内部セグメントに配備可能なサービスを提供する	○	-	-
		保存情報の機密性確保	保存されているデータの搾取を防止するため処置及び搾取された場合に影響を低減させるための、措置を行うこと。	通信制御可能な FW サービスを提供する	○	-	-
				VLAN で情報を保存する機器を内部セグメントに配備可能なサービスを提供する	○	-	-
		保存情報の完全性確保	情報が不正に改ざんさせることを防止するため、システムが取り扱う情報の完全性を確保すること。	改ざん検知ソフト又はサービスを提供する	○	-	-

対策区分	対策方針	対策要件	目的	対応方針	実施者		
					受注者	設計・開発業者	運用・保守業者
物理対策	情報搾取・侵入対策	侵入の物理的対策	物理的に区画させたエリアに不正に侵入しての不正行為を防止するための、措置を行うこと。	入退館管理やラック開錠・作業ルールの徹底されたデータセンター設備を提供すること	○	-	-
障害対策（事業継続対応）	構成管理	システムの構成管理	必要な機器のみによって必要なサービスのみを提供するように情報システムの構成及び稼働状況の管理を行うこと。	機器構成や稼働状況の把握が可能なサービスを提供すること	○	-	-
	可用性確保	システムの可用性確保	システムの異常停止を防止するとともに障害時のシステムの迅速な復旧を行うこと。	VPS 環境にて保有する HA サービスを提供すること	○	-	-
				IaaS にて機器、ネットワークの冗長化が行われていること	○	-	-
				システムバックアップ、データバックアップ保管サービスの提供が可能なこと	○	-	-
				定期的にシステムバックアップ、データバックアップを実施すること	-	-	○
				障害時にリストア作業を実施すること	-	-	○

別紙３：　バックアップ・リカバリ方針

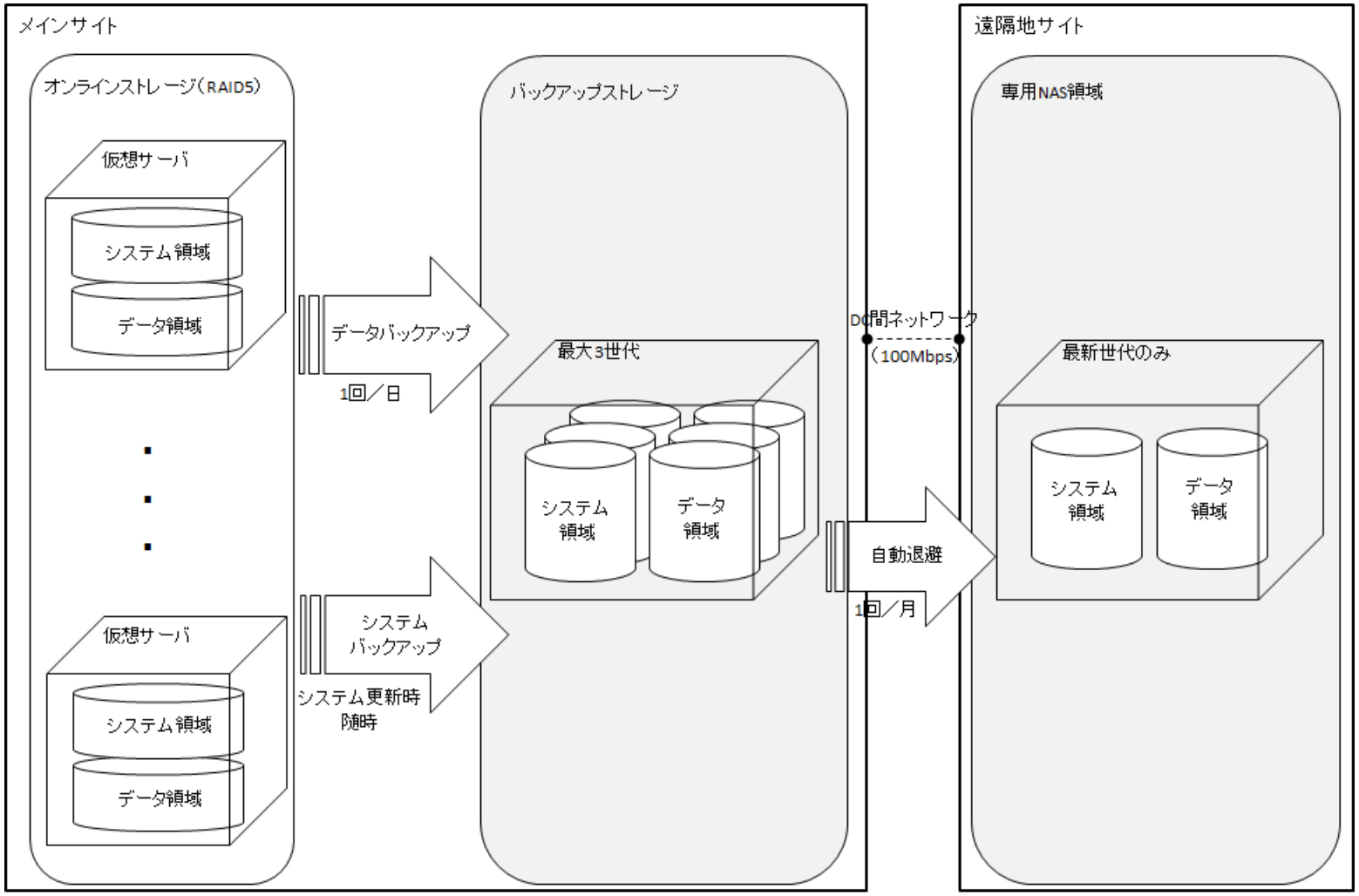
障害の種類	リカバリの考え方	目標復旧時点（RPO）	目標復旧時間（RTO）	バックアップデータの保管先	バックアップ方式の説明	バックアップ頻度と世代数
①HDD 障害時	（単独障害）　※HDD1 本の故障 ・RAID 構成により業務影響が発生しないこと。 ・ホットスペアにより自動的に RAID 構成が再構築されること。 ・ホットスワップにより業務を停止することなく HDD の交換が行えること。	障害発生時点	障害発生時点	ディスク内に保管 ※稼働環境とは別の領域に保管すること	RAID5 によるミラーリング	常時
	（多重障害）　※HDD2 本以上の故障 ・RAID グループを複数に分割にすることで、HDD の多重障害に対応する。ただし、同一 RAID グループ内で HDD の多重障害が発生した場合にはデータの損失が発生する。	障害発生時点	障害発生時点	ディスク内に保管 ※稼働環境とは別の領域に保管すること	RAID5 によるミラーリングと RAID グループの細分化	常時
②ユーザ障害障害時（ファイルの誤消去等、人為的なもの）	対応不要	－	－	－	－	－
③ディスク装置障害時	・障害部位の交換、HDD 再装填、ディスク装置の環境再設定等による対応が行えること。	障害発生時点	6 時間以内	－	－	－

障害の種類	リカバリの考え方	目標復旧時点(RPO)	目標復旧時間(RTO)	バックアップデータの保管先	バックアップ方式の説明	バックアップ頻度と世代数
④データ障害時(データベースファイル破損等)	・日次データバックアップからリカバリを行えること。 ※データバックアップの設定は設計・開発業者が行う ・データバックアップからのリカバリ後にアーカイブログ等から可能な限りデータの最新化が行える様に考慮すること。(運用保守作業) ≪データバックアップ対象≫ ・CMS サーバ:CMS 用データベース、コンテンツ更新履歴データ ・改ざん検知サーバ:コンテンツ(マスター) ・インタフェースサーバ:Oracle データベース(全文検索インデックス含む)、添付文書	障害発生時点	6 時間以内	オンラインストレージ上に保管 ※システム領域とは別の領域とすること	ディスク to ディスク	1 回/日 (データバックアップ:3 世代保管)
⑤システム障害時 (目標復旧時間:6 時間以内)	・クラウドサービスが提供する機能でシステムバックアップが取得できること。 ・バックアップ用のオンラインストレージ上に格納されたシステムバックアップからシステムのリストアが行えること。 ・システムのリストア後に、データバックアップからデータの最新化を行う。(運用保守作業)	1 週間以内	6 時間以内	オンラインストレージ上に保管 ※システム領域とは別の領域とすること	ディスク to ディスク	システム更新時等随時 (システムのフルバックアップ:3 世代保管)

障害の種類	リカバリの考え方	目標復旧時点(RPO)	目標復旧時間(RTO)	バックアップデータの保管先	バックアップ方式の説明	バックアップ頻度と世代数
⑥災害時 (データセンター被災や、職員が半数以上出勤できない時)	・週次で遠隔地にあるリモートサイトにバックアップデータの保管が行えること。 ・データセンター復旧後にバックアップデータからシステムの復旧を行う。(運用保守作業)	1ヶ月以内	1週間以内の再開を目標	リモートサイト(遠隔地)のストレージ上に保管	遠隔地保管	1回／月 (バックアップデータのフルバックアップ：1世代保管) ※リモートサイトへのバックアップ中にメインサイトで障害が発生しても最新のバックアップデータには影響がないこと。
⑦広域災害時 (災害時＋遠隔地保管先も被災した時)	・保守資料(設計書等)からシステムの復旧(再構築)が行えること。	－	－	－	－	

※システム障害：クラウドサービスで提供される VPS 等に障害が発生し、サーバの復旧作業が必要となる障害（IaaS 障害は含まない。）

（バックアップ概要）


メインサイト
オンラインストレージ（RAID5）
仮想サーバ
システム領域
データ領域
仮想サーバ
システム領域
データ領域
データバックアップ
1回／日
システム
バックアップ
システム更新時
随時
バックアップストレージ
最大3世代
システム
領域
データ
領域
DC間ネットワーク
（100Mbps）
自動退避
1回／月
遠隔地サイト
専用NAS領域
最新世代のみ
システム
領域
データ
領域

別紙４：　運用監視・保守方針と役割分担

作業区分	作業項目	作業内容	実施者		
			受注者	設計・開発業者	運用・保守業者
稼働業況管理	サービス管理	仮想サーバ、サービスの起動・停止・再起動のオペレータ作業サービスの提供	○	-	-
		仮想サーバ、サービスの起動・停止・再起動のオペレータ作業の実施	-	-	○
ストレージ管理	バックアップ	システムバックアップサービス、データバックアップ保管サービスの提供	○	-	-
		バックアップ設計・自動データバックアップ設定	-	○	-
		運用マニュアルに基づくデータ及びシステムイメージのバックアップの実施	-	-	○
		システムバックアップ管理票の作成、提供	-	-	○
	リストア	保守マニュアルに基づくデータ及びシステムイメージリストアの実施	-	-	○
		システムリストア管理票の作成、提供	-	-	○
ログ管理	ログチェック	ログ監視サービスの提供	○	-	-
		OS ログ、ミドルウェアログの運用監視設定	-	○	-
		監視対象ログの確認	-	-	○
ユーザ管理	OS　ID 管理	管理者・運用担当者のログイン ID、パスワードの発行	-	-	○
		管理者等の権限変更への対応	-	-	○
		管理者・運用担当者の登録情報変更への対応	-	-	○

作業区分	作業項目	作業内容	実施者		
			受注者	設計・開発業者	運用・保守業者
問合わせ管理	照会対応	サービスデスク（IaaS 監視、障害対応）を提供すること	○	-	-
セキュリティ管理	パッチ適用	セキュリティパッチ（OS）アップデート環境の提供	○	-	-
		事前検証サーバにおけるパッチ適用及び検証	-	-	○
		本番環境へのセキュリティパッチ（OS）の適用	-	-	○
		本番環境へのセキュリティパッチ（ミドルウェア）の適用	-	-	○
		パッチの適用状況管理	-	-	○
	ウイルスパターンファイル更新	パターンファイルの更新（自動／手動）	○	-	-
		パターンファイルの更新状況管理	-	-	○
	侵入検知	外部からの侵入に対するセキュリティ監視	○	-	-
	ウィルス監視	ウィルス除去・検知に対する監視	○	-	-
稼働状況管理	死活監視	クラウドセンターに設置した仮想サーバ等を対象とした死活監視（Ping）	○	-	-
	閾値監視	CPU/メモリ/ディスクの閾値監視	○	-	-
		データベースの空き容量監視	○	-	-
	サービス・プロセス稼働監視	サービス稼働監視（ポート番号単位）	○	-	-
		アプリケーション稼働上必要なプロセスの監視	○	-	-
	通知・閲覧	アラート通知	○	-	-

作業区分	作業項目	作業内容	実施者		
			受注者	設計・開発業者	運用・保守業者
		イベント通知	○	-	-
		性能情報蓄積/閲覧	○	-	-
構成管理	ハードウェア・ソフトウェア構成管理	システムを構成するサーバー一覧、サーバ導入ソフトウェア構成等をまとめ、変更が生じた場合は反映させる	-	-	○
保全管理	障害対応	各担当ベンダーから提供されるサービス等に関するインシデント情報の取り纏め管理	-	-	○
物品管理	ドキュメント管理	クラウド環境構築で作成したマニュアル等のドキュメントを保管	-	-	○
報告関連	システム運用報告（月次）	運用報告書に必要となる監視情報の蓄積、閲覧サービスの提供	○	-	-
		システム運用報告書（月次）に、当月の業務実施状況について取りまとめ、提出する	-	-	○
	改善状況報告	IaaS 障害の原因分析及び改善策について必要に応じて報告する	○	-	-
		IaaS 以外の障害の原因分析及び改善策について必要に応じて報告する	-	-	○
保守窓口	保守窓口	ソフトウェア、ハードウェア、クラウドサービスの製品保守サービスの取得	○	-	-
		システム運用支援期間中の各種製品、クラウドサービスの保守サービスベンダーとの窓口対応	○	-	-
		保守サービスの更新	○	-	-